IN THE SPECIFICATION

1. Please amend the paragraph [0021] of page 4 as follows:

[0021] Now making reference to the drawings, FIG. 1 illustrates the preferred embodiment of the invention in the form of a portable ~~smartcards reader~~ device 100, with a smartcard reader indicated generally at 101 ~~100~~. The device includes slot(s) 102 to receive the card 104, and a keyboard 110 enabling passwords, personal identification numbers, and the like to be input by a user. It will be appreciated that although a generic "smartcard" is shown in the figure, in the preferred embodiment, the unit includes its own central-processing unit for transaction management and input/output capability for reading and writing information to various other types of cards including magnetic cards, optical cards, EAROM cards, random-access memory (RAM) cards, and read-on memory (ROM) cards. Nor is the unit limited to the use of a single type of smartcard or other card, since in alternative embodiments, the same unit may recognize multiple card owners and users.

2. Please amend the paragraph [0042] of page 11 as follows:

[0042] After the smartcard and/or reader performs appropriate public key authentications and validation of digital signature, the encrypted data is sent back to the DTMF encoder/decoder, enabling the phone, computing device or other unit to validate the authentication transaction. In terms of security, each transaction uses its own encrypted counter with signals that are different to prevent recording thanks to the usage of atomic clock component at the synchronization level. Within the reader 101~~100~~, the software is preferably stored in an

obfuscated manner, with each module being preferably software encrypted and decrypted and re-encrypted after usage using a unique process, with new sessions keys being transmitted to prevent disassembly or decompilation of the software or portions thereof. Sensors within the unit may be used to detect excessive use of heat or power, representing some form of misconduct which would be reported during the next transaction with all information needed to prevent further usage.